



THE
TECHNOLOGY
PROVIDER

TECH& SNACK



FortiOS 7.4 – What's New?

30.Juni in Emmen



WER WIR SIND



**Andreas (Andi)
Tischer**

Channel PreSales Engineer
Fortinet Schweiz



**Martin (Tinu)
Ruesch**

Tech. Consultant Security
ALSO Schweiz



**Cvijetin (Chris)
Tanasic**

Tech. Consultant Security
ALSO Schweiz



**Guido
Handel**

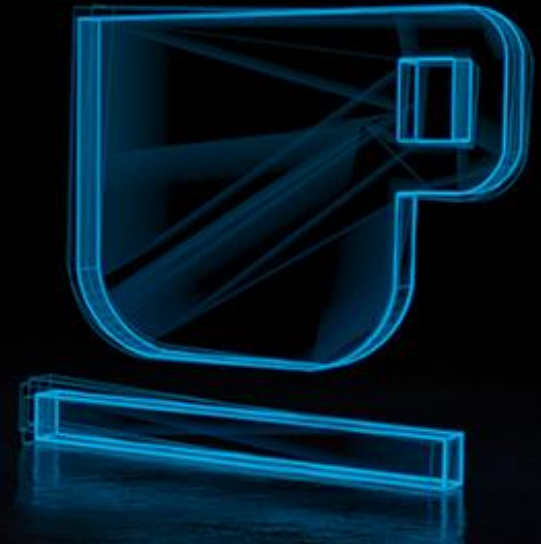
OT Security System Engineer
Fortinet Schweiz

WAS EUCH HEUTE ERWARTET

- ▶ Neues Produkt – FortiGate 900/901G
- ▶ Hinweis FortiOS 6.2
- ▶ Was gibt es Neues im FortiOS 7.4?
- ▶ Agora Community
- ▶ Fragen

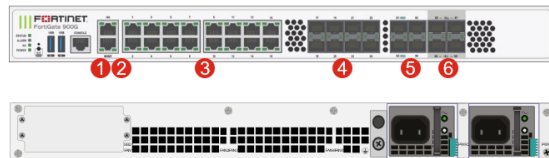
ALSO & FORTINET

Tech & Snack











NEUES PRODUKT – FORTIGATE 900/901G

FortiGate 900/901G

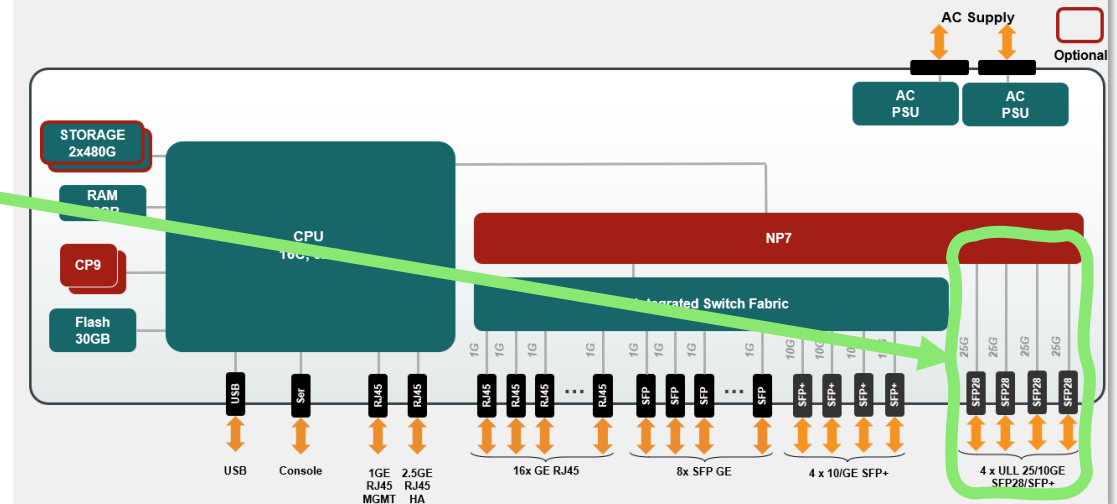


- ① 1x GE RJ45 Management Port
- ② 1x 2.5GE RJ45 HA Port
- ③ 16x GE RJ45 Ports
- ④ 8x GE SFP Slots
- ⑤ 4 x 10GE/GE SFP+/SEF Slot
- ⑥ 4 x 25GE/10GE SFP28/SFP+ ULL (ultra-low latency) Slots











 164 Gbps Firewall throughput	 26 Gbps IPS Throughput	 Enterprise Branch / Mid Enterprise NGFW / Secure SD-WAN / IPS / SWG
 720,000 New Sessions/Sec	 22 Gbps NGFW Throughput	
 16.7 Gbps SSL Inspection Throughput	 20 Gbps Threat Protection Throughput	
 5,000  1,024  96		

FortiGate 900/901G Schematic



FORTIOS 6.2 – GEHT END-OF-SUPPORT (28.9.23)

- ▶ FortiOS wird Ende September 2023 **End of Support** gehen (EoS)
- ▶ Upgraden auf eine supportete Version
- ▶ Upgrade Pfad beachten! 
- ▶ Infos in unserem WIKI:

Software Version	Release Date (GA)	End of Engineering Support Date (EOES)	End of Support Date (EOS)
6.0 	29.03.2018	29.03.2021	29.09.2022
6.2 	28.03.2019	28.03.2022	28.09.2023 
6.4 	31.03.2020	31.03.2023	30.09.2024
7.0 	30.03.2021	30.03.2024	30.09.2025
7.2 	31.03.2022	31.03.2025	30.09.2026
7.4 	11.05.2023	11.05.2026	11.11.2027

- ▶ Offizieller Lifecycle:
<https://support.fortinet.com/Information/ProductLifeCycle.aspx>

Release Notes

Download

Upgrade Path

FortiGate Support Tool

FortiOS Version Upgrade Path

Current Product:
FortiGate-100F

Current FortiOS Version:
6.2.15

Upgrade To FortiOS Version:
7.4.0

Upgrade information for older FortiOS versions (before 5.2.9) can be found [here](#).

GO

Recommended Upgrade Path

Following is the recommended FortiOS migration path for your product.

Version	Build Number
6.2.15	1378
6.4.13	2092
7.0.12	0523
7.2.5	1517
7.4.0	2360



WAS GIBT ES NEUES IM FORTIOS 7.4?



PLATFORM SUPPORT – FORTIOS 7.4.0

	7.0.12	7.2.5	7.4
FG/FWF-60E/80E/90E	●	●	●
FG/FWF-40F Series	●	●	●
FG/FWF-60F Series	●	●	●
FG-70F Series	●	●	●
FG-80E Series	●	●	●
FG/FWF-80F Series	●	●	●
FG-100/101E Series	●	●	no
FG-100F Series	●	●	●
FG-200/201E	●	●	●
FG-200F	●	●	●
FG-400F/600F Series	●	●	●
FG-400E/600E Series	●	●	●
FG-900G Series	*	??	??
FG-1500D Series	●	●	no

* es existiert ein Special Brand im 7.0.10 Build 6607

	7.0.12	7.2.5	7.4
FG-1100E Series	●	●	●
FG-1000F Series	#	●	7.4.1
FG-1800F Series	●	●	●
FG-2200E, 3300E Series	●	●	●
FG-2000E, 2500E	●	●	●
FG-2600F Series	●	●	●
FG-3000F Series	●	●	Geplant
FG 3200F Series	#	Geplant	7.4.x
FG-3400E/3600E	●	●	●
FG-3500F Series	●	●	●
FG-3700F Series	#	Geplant	7.4.x
FG-4200/4400F Series	●	●	●
FG-4800 Series	#	7.2.6	7.4.1

Special Brand vorhanden (siehe Release Notes)

PLATFORM SUPPORT – FORTIOS 7.4.0

Supported models

FortiOS 7.4.0 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-70F, FG-71F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100F, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-400F, FG-401F, FG-500E, FG-501E, FG-600E, FG-601E, FG-600F, FG-601F, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3000F, FG-3001F, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-5001E, FG-5001E1, FG-6000F, FG-7000E, FG-7000F
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-60F, FGR-60F-3G4G, FGR-70F, FGR-70F-3G4G
FortiFirewall	FFW-3980E, FFW-VM64, FFW-VM64-KVM
FortiGate VM	FG-ARM64-AWS, FG-ARM64-AZURE, FG-ARM64-GCP, FG-ARM64-KVM, FG-ARM64-OCI, FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VM64-XEN

FortiGate 6000 and 7000 support

FortiOS 7.4.0 supports the following FG-6000F, FG-7000E, and FG-7000F models:

The hardware models listed below do not support FortiOS version 7.4:

FortiGate 100E, 101E, 100EF, 1500D, 1500DT. Access to Fortinet Customer Services for support on 7.2 is available for these hardware models until they reach their hardware End-of-Support date.

FORTI AP KOMPATIBILITÄT

- ▶ Folgende APs werden vom FortiOS 7.4 unterstützt:
 - ▶ FortiAP E-Serie
 - ▶ FortiAP F-Serie
 - ▶ FortiAP G-Serie
 - ▶ APs müssen mindestens FortiOS 7.2.2 installiert haben!
- ▶ Modelle der **Serie B, C und D** werden **nicht** mehr vom FortiOS 7.4.0 unterstützt

FortiOS 7.4.x compatibility


FortiAP	FortiOS Versions
	7.4.0
Wi-Fi 6 Models	
FAP-23JF	7.4.0
FAP-231F	7.4.0
FAP-234F	7.4.0
FAP-431F	7.4.0
FAP-432F	7.4.0
FAP-433F	7.4.0
FAP-831F	7.4.0
Wi-Fi 6E Models	
FAP-231G	7.4.0
FAP-233G	7.4.0
FAP-431G	7.4.0
FAP-433G	7.4.0




FortiGates running FortiOS version 7.4.0 do not support legacy FortiAP models (B, C and D series).

BEZEICHNUNG FEATURE / MATURE

- **Feature** : Patch enthält neue Features und Bugfixes. Wird durch ein **F** markiert:

 FGT_100F-v7.0.8.**F**-build0418-FORTINET.out

- **Mature** : Patch enthält Bugfixes, keine neuen Features werden hinzugefügt. Wird durch ein **M** markiert.

 FGT_100F-v7.0.12.**M**-build0523-FORTINET.out

- Für produktive Systeme empfehlen wir ausschliesslich **Mature Patches** zu installieren

7.0.11 Mature	FortiOS v7.0.11 build0489 (GA) Release notes Security Fabric upgrade notes
7.0.10 Mature	FortiOS v7.0.10 build0450 (GA) Release notes Security Fabric upgrade notes
7.0.9 Mature	FortiOS v7.0.9 build0444 (GA) Release notes Security Fabric upgrade notes
7.0.8 Feature	FortiOS v7.0.8 build0418 (GA) Release notes Security Fabric upgrade notes
7.0.7 Feature	FortiOS v7.0.7 build0367 (GA) Release notes Security Fabric upgrade notes



NEUES IM WEBGUI – DASHBOARD – LIVE DEMO

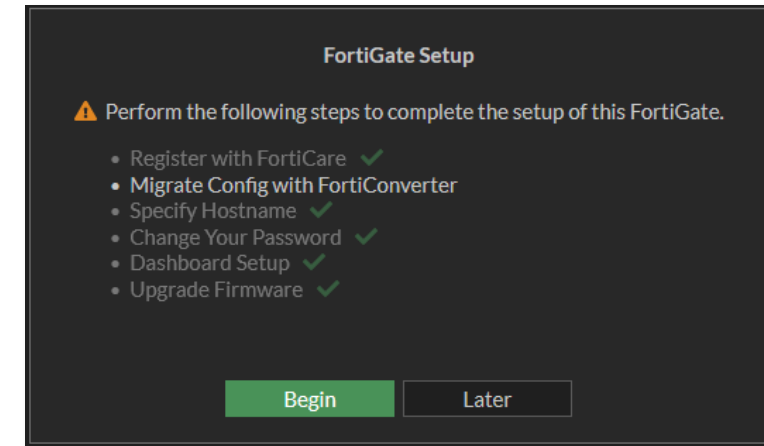
WEBGUI: INTEGRIERTER FORTI CONVERTER SERVICE

► Kostenpflichtiger Service

- Im Enterprise Bundle inkludiert
- A la Carte Service: FC-10-**0060F**-189-02-DD
0060F Zielsystem (siehe Datenblatt)
- Lizenz muss auf dem Zielsystem gelöst sein

► Konvertieren mit Backupfile der Source FortiGate

► Konvertieren direkt von der Source FortiGate mit eingeschalteter Option



Start Up Settings

Allow FortiConverter to obtain config file once ☒

Auto file system check ☐

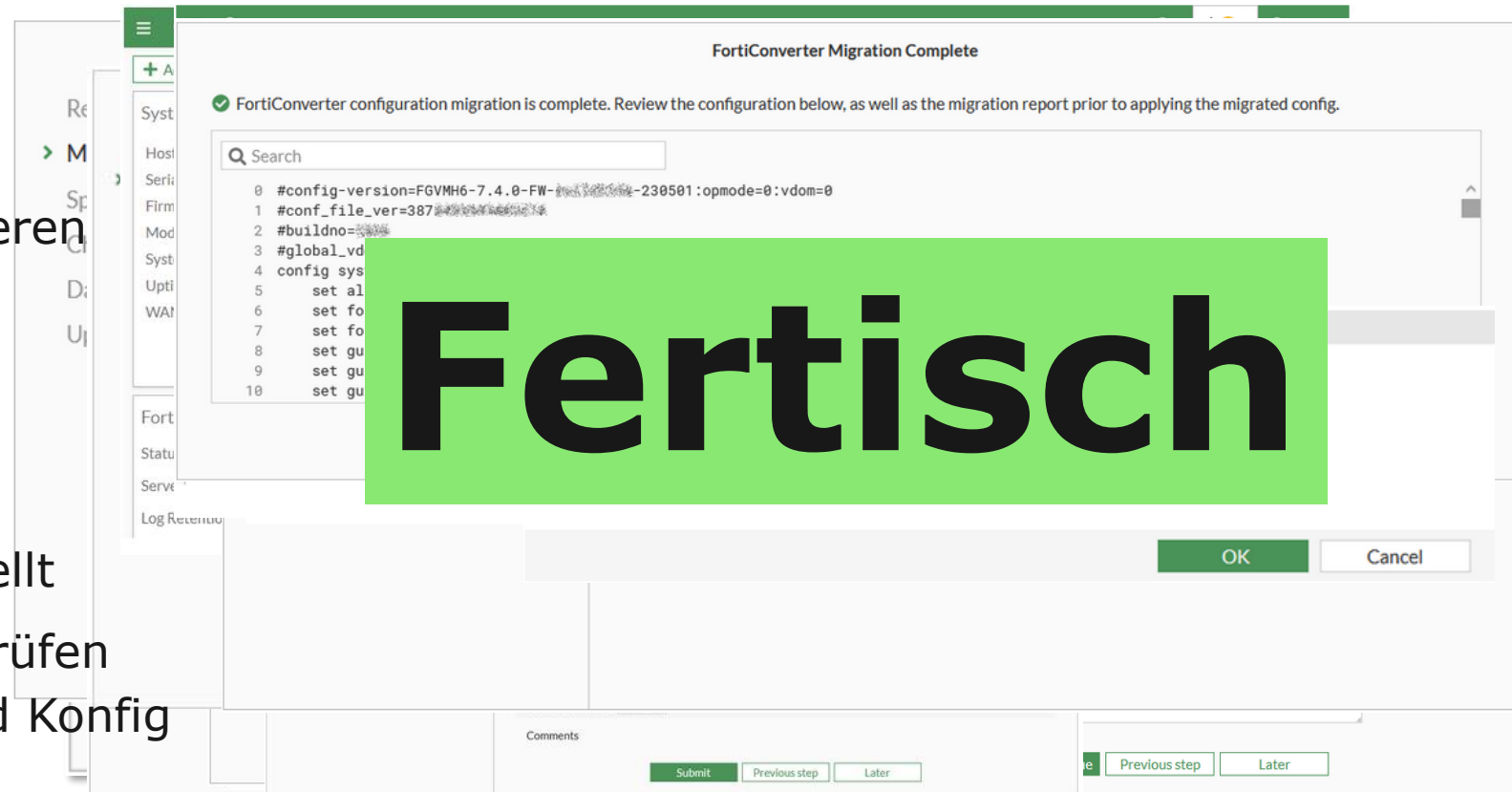
USB auto-install ☐

Detect configuration ☐

Detect firmware ☐

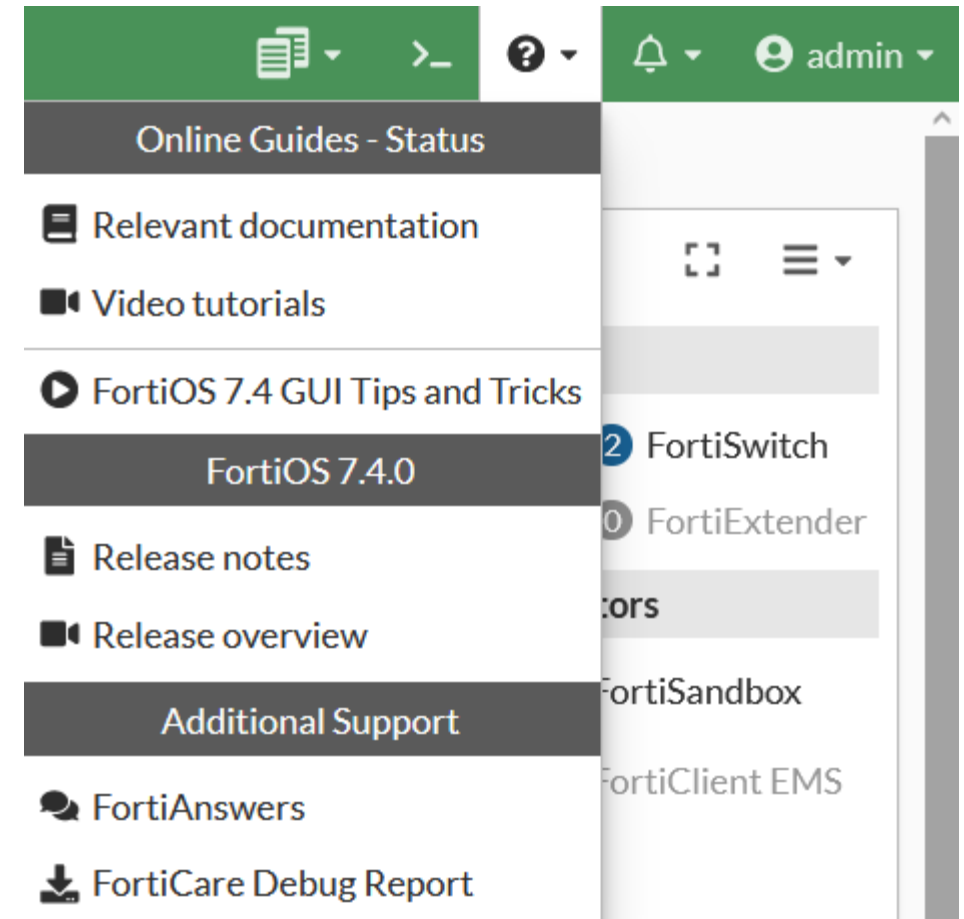
FORTI CONVERTER IM ZEITRAFFER

- ✓ Mit Begin Wizard starten
- ✓ Source der Konfig definieren
- ✓ Konfiguration wird hochgeladen
- ✓ Interface Mappings definieren
- ✓ Eventuell MGMT Interface definieren
- ✓ Kontakt Informationen angeben
- ✓ Einstellungen überprüfen
- ✓ Bestätigen und Prozess starten
- ✓ Ticket erstellt mit Ticketnummer
- ✓ Bestätigungs E-Mail wird zugestellt
- ✓ Aktuellen Status im Menu überprüfen
- ✓ Wenn komplett, kann Report und Konfig File heruntergeladen werden
- ✓ Bestätigungs E-Mail sobald Konvertierung fertig ist
- ✓ Notifikation im Menu → Download des Reports und der Konfig → Konfig File einspielen



WEBGUI: ZUSÄTZLICHE UNTERSTÜTZUNG

- ▶ Überarbeitetes Hilfe Menu
- ▶ Direkter Zugriff zu Release Notes
- ▶ Direkter Zugriff zu FortiAnswers
- ▶ TAC Report für L1 Tickets
- ▶ Kommando Palette `ctrl+p` (mac: `cmd+p`)

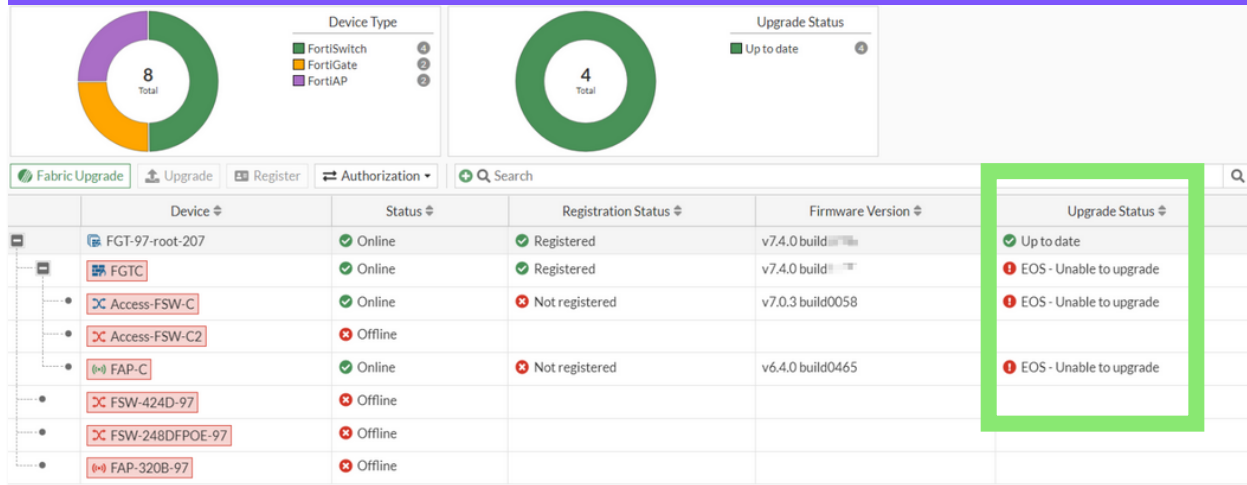




NEUE FEATURES BEIM UPDATEN

WARNUNG FÜR HARDWARE MIT EOS DATUM

Menu: System → Firmware & Registration



Device has reached End of Support (EOS) status. Please replace with a supported device to receive updates.

FortiGate	FGTC
Hostname	FGTC
Serial Number	FG101ETK18
Authorization Type	Serial Number
Model	FortiGate 101E
Version	v7.4.0 build
Operation Mode	NAT
Management IP/FQDN	robot_securityfabric_qa_fortinet.com
Management Port	4433
CPU Usage	34%
Memory Usage	34%
Session Count	63

Firmware Version	Upgrade Status
v7.4.0 build	EOS - Unable to upgrade
v7.0.3 build0058	EOS - Unable to upgrade
v6.4.0 build0465	EOS - Unable to upgrade

AUTOMATISCHE UPDATES

- ▶ Führt automatisch einen Software Update aus (Parameter können in der CLI konfiguriert werden)
- ▶ Führt Updates nur im selben GA Range aus
 - ▶ Update : **7.4.0** → **7.4.1** (Update wird ausgeführt)
 - ▶ Update : **7.4.5** → **7.6.0** (Update wird nicht ausgeführt, da neuer GA Release)
- ▶ Nach dem Update wird ein E-Mail an die FortiCloud Account Adresse gesendet

```
config system fortiguard
  set auto-firmware-upgrade {enable | disable}
  set auto-firmware-upgrade-day {sunday monday tuesday wednesday thursday friday saturday}
  set auto-firmware-upgrade-delay <integer>
  set auto-firmware-upgrade-start-hour <integer>
  set auto-firmware-upgrade-end-hour <integer>
end
```

UPDATE MIT INAKTIVEM FORTICARE

- ▶ Upgrade ab 7.4.0 auf Major oder Minor Release nur noch mit aktiver FortiCare Lizenz möglich
 - ▶ Update im aktuellen Patchpfad wie z.B. **7.4.0** auf **7.4.5** ist möglich
 - ▶ Update auf Major Release wie z.B. **7.4.8** auf **7.6.0** ist nicht mehr möglich
- ▶ Auch bis anhin darf nur upgedatet werden, wenn eine aktive/gültige FortiCare Lizenz auf dem Gerät vorhanden ist !

Menu: System → FortiGuard

License Information

Entitlement	Status
+ FortiCare Support	✓ Registered
+ Virtual Machine	✓ Valid (Expiration Date: 2024/06/13)
+ Firmware & General Updates	✓ Licensed (Expiration Date: 2024/06/14)

```
diagnose test update info contract
```

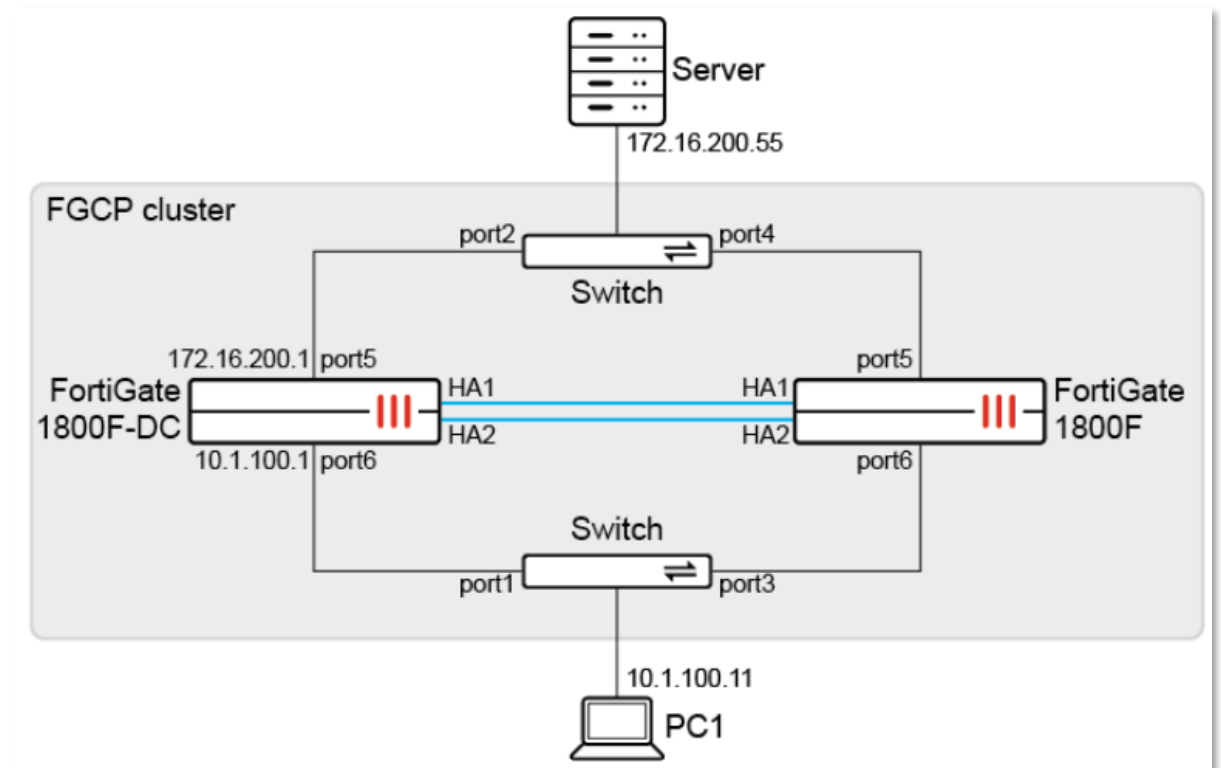


NEUERUNGEN IM HA



FORTIGATE HA MIT DIV AC- UND DC-NETZTEILEN

- ▶ Clusterbildung möglich mit dem selben FortiGate Modell aber unterschiedlichen PSUs Setups
- ▶ Clusterbedingungen:
 - ▶ Gleiches Modell
 - ▶ Gleiche Firmware
 - ▶ Selbe Hardware Konfiguration (Ausnahme: Netzteil)
- ▶ Beispiel:
 - ▶ FortiGate 1800F-**DC** (primär) und FortiGate 1800F (sekundär)

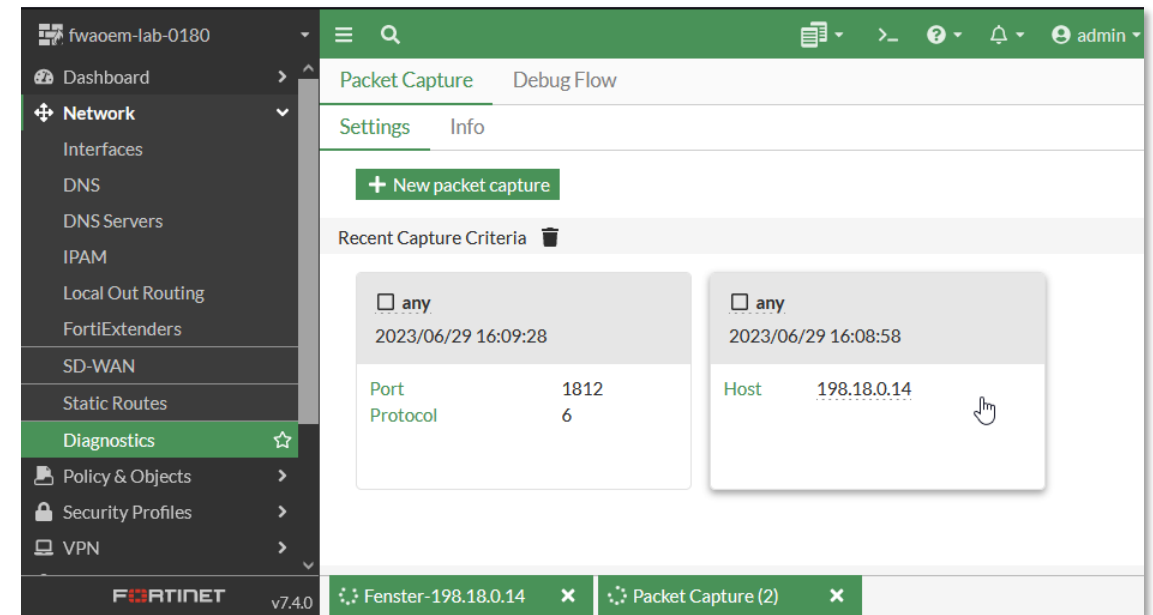




TROUBLESHOOTING PACKET SNIFFER – LIVE

MEHRERE PACKET SNIFFER IM WEBGUI

- ▶ Es können gleichzeitig mehrere Packet Sniffer Fenster aktiv sein
- ▶ Weiteres Navigieren auf der FortiGate möglich (z.B. Policy deaktivieren, und Auswirkung im Sniffer beobachten)
- ▶ Fenster können benannt werden



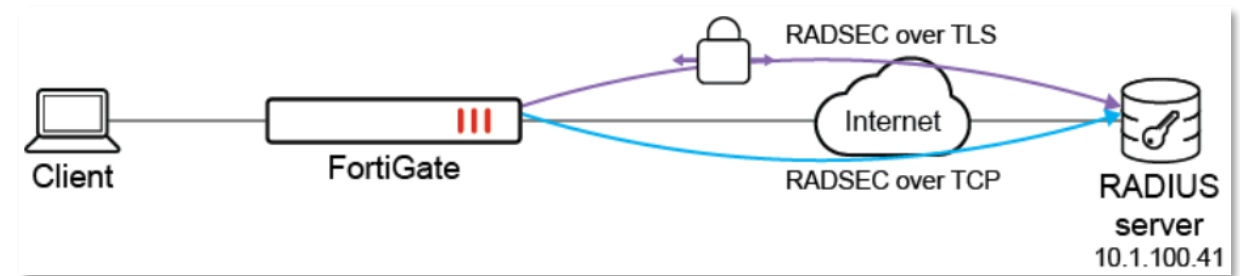


NEUERUNG BEI DER USER AUTHENTIFIZIERUNG

RADSEC CLIENT SUPPORT

► Transport Protokoll

- UDP: Default UDP (udp1812)
- TCP: TCP ohne TLS (Auth: tcp1812 Acc: tcp1813)
- TLS: TLS over TCP (Auth/Acc: tcp2083)




```
config user radius
  edit <name>
    set transport-protocol {udp | tcp | tls}
    set ca-cert <string>
    set client-cert <string>
    set tls-min-proto-version {default | SSLv3 | TLSv1 | TLSv1-1 | TLSv1-2}
    set server-identity-check {enable | disable}
  next
end
```



NEUE FEATURES BEI DEN POLICIES

WO IST DER PROXY MODUS IM WEBGUI?

- ▶ Bei kleineren Geräten (<100F) ist nur noch der Flow Modus im WebGUI aktiviert

☐ Explicit Proxy 

Enable an HTTP, HTTPS, or FTP proxy for your network and add the proxy to one or more FortiGate interfaces. Users on your network must configure their browsers to use the proxy. Set up the explicit proxy under Network > Explicit Proxy. Create security policies to control access to the proxy and apply UTM and other features to proxy traffic.

Must be enabled via CLI first:

```
config system global
  set proxy-and-explicit-proxy enable
end

config system settings
  set gui-proxy-inspection enable
end
```

Incoming Interface	<input type="text"/>
Outgoing Interface	<input type="text"/>
Source	<input type="text"/>
Destination	<input type="text"/>
Schedule	<input type="text" value="always"/>
Service	<input type="text"/>
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY

Firewall/Network Options

NAT

☒

IP Pool Configuration

☒ Use Outgoing Interface Address ☐ Use Dynamic IP Pool

Preserve Source Port

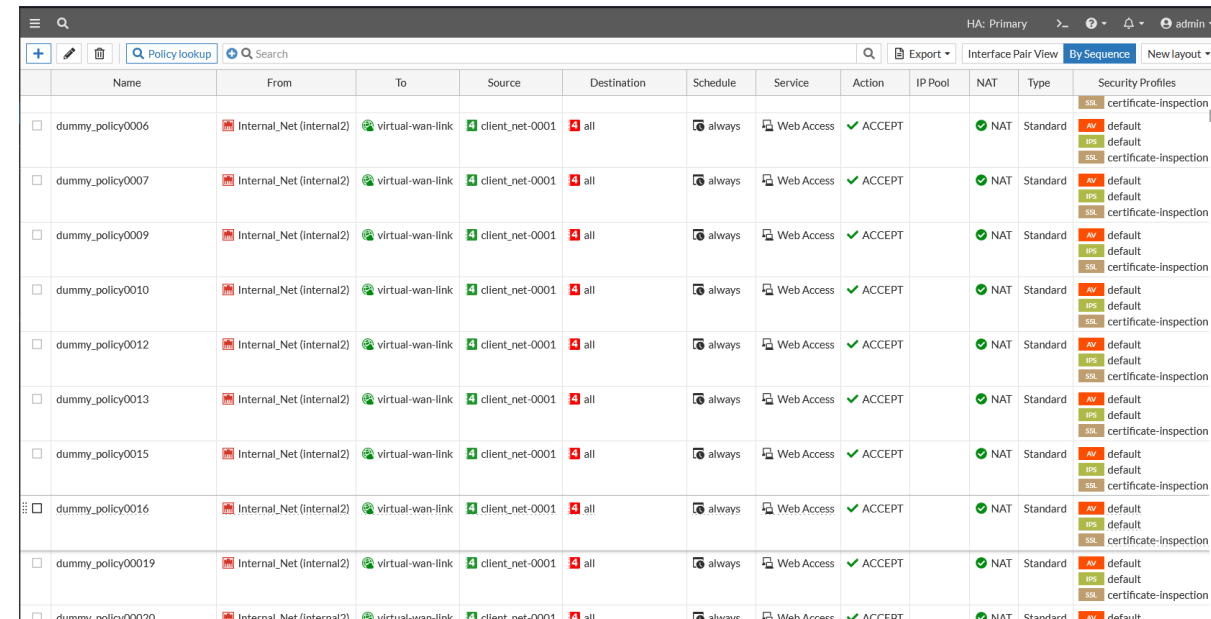
☐

- ▶ Über die CLI wieder aktivieren

```
config system setting
  set gui-proxy-inspection enable
end
```

ÜBERARBEITETES POLICY MANAGEMENT

- ▶ Auswahl zwischen klassischem und neuem Layout
- ▶ Neues Layout:
 - ▶ Mehrfach-Selektion möglich
 - ▶ Gleichzeitige Änderungen in verschiedenen Regeln möglich (z.B. Source Interface ändern)
 - ▶ Für grosse Regelwerke konzipiert
- ▶ Es kann jederzeit zwischen den beiden Layouts gewechselt werden



The screenshot displays the FortiOS Policy Management interface. At the top, there's a search bar and navigation tabs. Below, a table lists policies with columns for Name, From, To, Source, Destination, Schedule, Service, Action, IP Pool, NAT, Type, and Security Profiles. The table contains 12 rows of dummy policies, each with a checkbox for selection. The 'From' column shows 'Internal_Net (Internal2)' and the 'To' column shows 'virtual-wan-link'. The 'Source' column shows 'client_net-0001' and the 'Destination' column shows 'all'. The 'Schedule' column shows 'always' and the 'Service' column shows 'Web Access'. The 'Action' column shows 'ACCEPT'. The 'IP Pool' column is empty. The 'NAT' column shows 'NAT'. The 'Type' column shows 'Standard'. The 'Security Profiles' column shows 'AV default', 'IPS default', and 'SSL certificate-inspection'.

	Name	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT	Type	Security Profiles
<input type="checkbox"/>	dummy_policy0006	Internal_Net (Internal2)	virtual-wan-link	client_net-0001	all	always	Web Access	ACCEPT		NAT	Standard	AV default IPS default SSL certificate-inspection
<input type="checkbox"/>	dummy_policy0007	Internal_Net (Internal2)	virtual-wan-link	client_net-0001	all	always	Web Access	ACCEPT		NAT	Standard	AV default IPS default SSL certificate-inspection
<input type="checkbox"/>	dummy_policy0009	Internal_Net (Internal2)	virtual-wan-link	client_net-0001	all	always	Web Access	ACCEPT		NAT	Standard	AV default IPS default SSL certificate-inspection
<input type="checkbox"/>	dummy_policy0010	Internal_Net (Internal2)	virtual-wan-link	client_net-0001	all	always	Web Access	ACCEPT		NAT	Standard	AV default IPS default SSL certificate-inspection
<input type="checkbox"/>	dummy_policy0012	Internal_Net (Internal2)	virtual-wan-link	client_net-0001	all	always	Web Access	ACCEPT		NAT	Standard	AV default IPS default SSL certificate-inspection
<input type="checkbox"/>	dummy_policy0013	Internal_Net (Internal2)	virtual-wan-link	client_net-0001	all	always	Web Access	ACCEPT		NAT	Standard	AV default IPS default SSL certificate-inspection
<input type="checkbox"/>	dummy_policy0015	Internal_Net (Internal2)	virtual-wan-link	client_net-0001	all	always	Web Access	ACCEPT		NAT	Standard	AV default IPS default SSL certificate-inspection
<input type="checkbox"/>	dummy_policy0016	Internal_Net (Internal2)	virtual-wan-link	client_net-0001	all	always	Web Access	ACCEPT		NAT	Standard	AV default IPS default SSL certificate-inspection
<input type="checkbox"/>	dummy_policy0019	Internal_Net (Internal2)	virtual-wan-link	client_net-0001	all	always	Web Access	ACCEPT		NAT	Standard	AV default IPS default SSL certificate-inspection
<input type="checkbox"/>	dummy_policy0020	Internal_Net (Internal2)	virtual-wan-link	client_net-0001	all	always	Web Access	ACCEPT		NAT	Standard	AV default IPS default SSL certificate-inspection



NEUERUNGEN IM SSL-VPN

SSL-VPN LANDINGPAGE ÜBERARBEITET

- ▶ Neues Layout auf der Landingpage
- ▶ Farbthemen können pro User unabhängig des globalen Farbschemas ausgewählt werden
- ▶ Einfache, private Bookmarks können erstellt werden

SSL-VPN Whats New 7.4

Powered by **FORTINET**

Quick Connection Settings

Protocol type HTTP/HTTPS

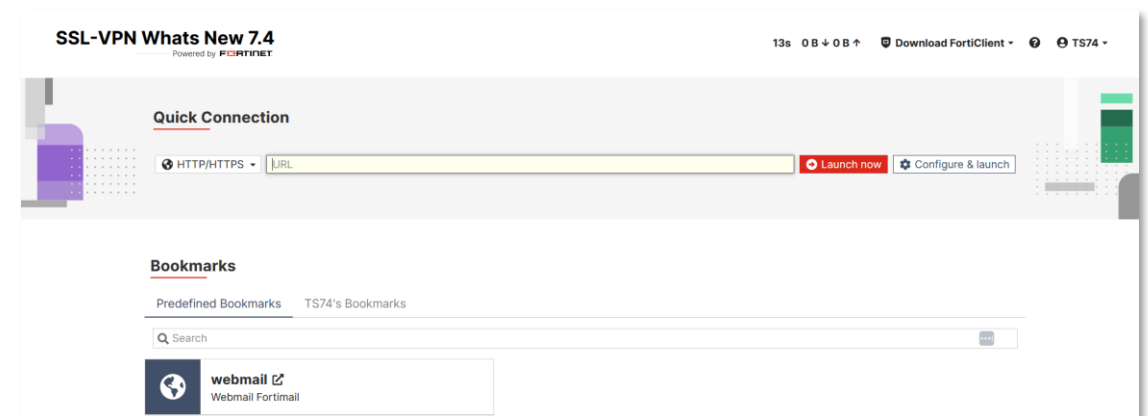
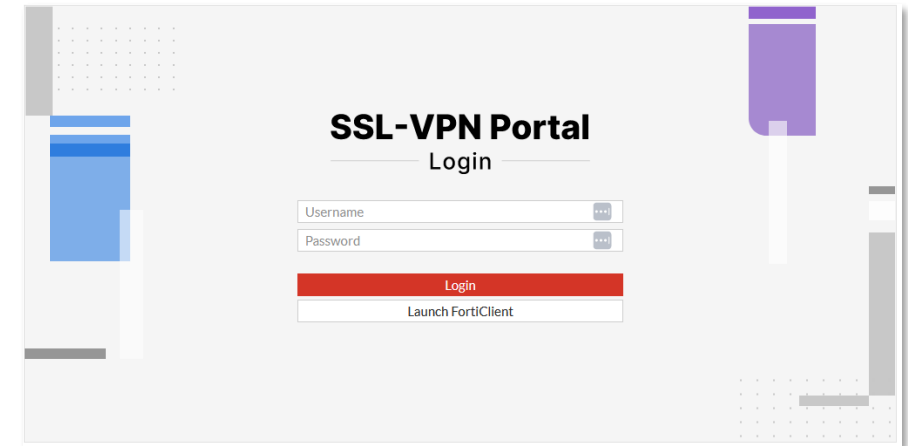
URL https://198.18.0.12:4443

SSO credentials ☐

☒ Save as bookmark after launching

Name FortiAnalyzer

Description FortiAnalyzer ALSO Demo Umgebung



SSL-VPN – REDIRECT AUF EIGENES PORTAL

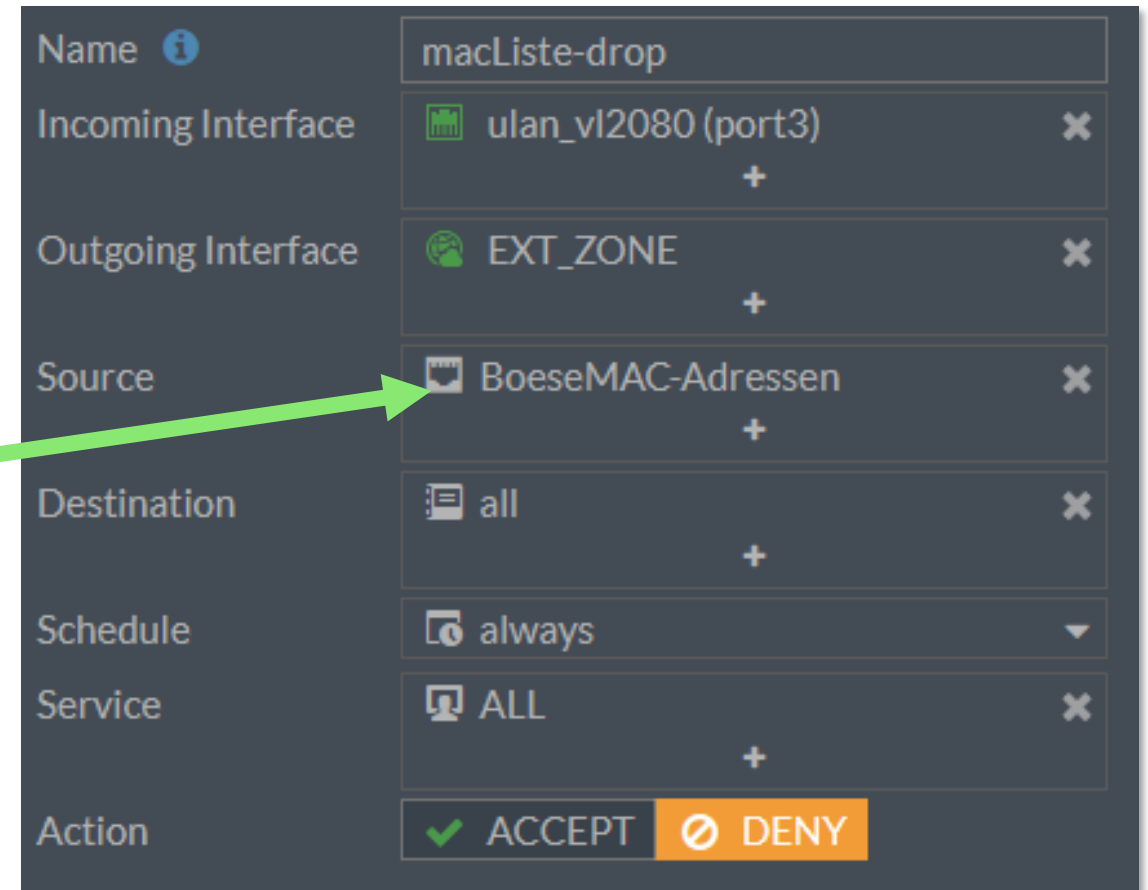
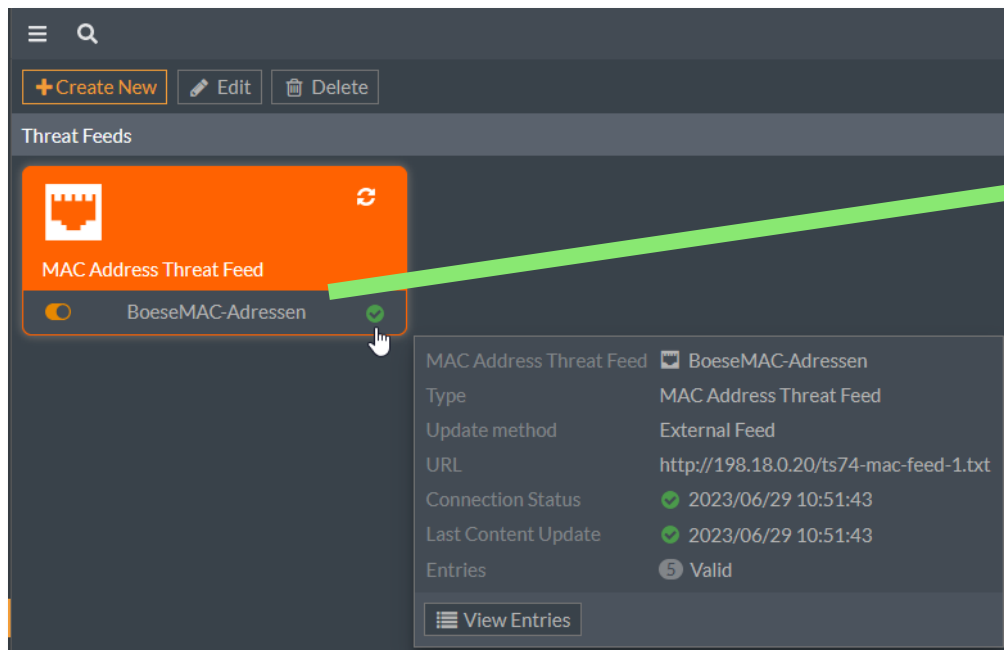
- Es kann auf eigene Landing Page nach dem Authentifizieren geleitet werden



FABRIC SETTING UND KONNEKTOREN – LIVE

MAC FEED – MIT POLICY

- ▶ Externe MAC Adressen Liste wird eingelesen
- ▶ Dynamisches Adress Objekt wird erstellt
- ▶ Kann in Firewall Regeln als Source/Destination Objekt verwendet werden



STITCHES DIREKT AUS EVENT LOG ERSTELLEN

- Aus dem Event Log kann direkt ein Trigger konfiguriert werden (erspart mühsames Suchen in der Liste)

2023/06/23 00:00:01	■■■ ■■■■	FortiManager Cloud Account Level license will expire in 3 day(s)	FortiManager Cloud Account Level license expi...
2023/06/23 00:00:00	■■■ ■■■■	System deleted log file tlog.65179	Disk log file deleted

Filter by Message

+ Create Automation Trigger

- Neue Aktionen:

System Action 3	
Backup Config Disk	ACTN Backup configuration
Reboot FortiGate	ACTN Reboot
Shutdown FortiGate	ACTN Shutdown

Create New Automation Trigger

FortiOS Event Log

A specified FortiOS event log ID has occurred.

Name

fmg_cloud_alert

Description

0/255

FortiOS Event Log

Event

FortiManager Cloud Account Level

+

Field filter(s)

+

Event

FortiManager Cloud Account Level licen...

ID

20131

Name

LOG_ID_FMGC_ACC_LIC_EXPIRE



FORTISWITCH – FEATURES 7.4 UND 7.2.4

FORTISWITCH – SERIENUMMER – ALIAS 7.2.4 ▲

- ▶ Gewisse Konfigurationen müssen in der CLI der FortiSwitches durchgeführt werden
- ▶ In der CLI muss bis anhin mit der Seriennummer auf den entsprechenden Switch verbunden werden
- ▶ Neu kann ein Name für den Switch definiert werden, welcher dann in der CLI angesprochen wird

```
config switch-controller managed-switch  
rename <SN/NR> to <NAME>
```

POE PORT SETTINGS 7.2.4

► Port Mode

- Strom nach IEEE Standard verteilt (Watt)
- IEEE802.3 AF = 15W* (12.95W**)
- IEEE802.3 AT = 30W* (25.5W**)
- IEEE 802.3BT = 90W* (71.3W**)

* Ausgangsleistung

** Leistung am Endgerät

► Port Priorität

- Strom wird nach Priorität verteilt

► Port Power


- Momentan nur auf 1xxE/1xxF Modellen
- Perpetual: Bei Soft-Reboot noch Strom
- Perpetual-fast: Bei Hard-Boot noch Strom

```
config switch-controller managed-switch
  edit <FortiSwitch_serial_number>
    config ports
      edit <port_name>
        set poe-port-mode {IEEE802_3AF | IEEE802_3AT | IEEE802.3 BT}
        set mpoe-port-priority {critical-priority | high-priority | low-priority }
        set poe-port-power {normal | perpetual | perpetual-fast}
      next
    end
  next
end
```


-
- ```

graph LR
 VD[Vulnerable device] ---|Port13| FS[FortiSwitch]
 FS ---|FortiLink| FG[FortiGate]
 FG --- I((Internet))

```

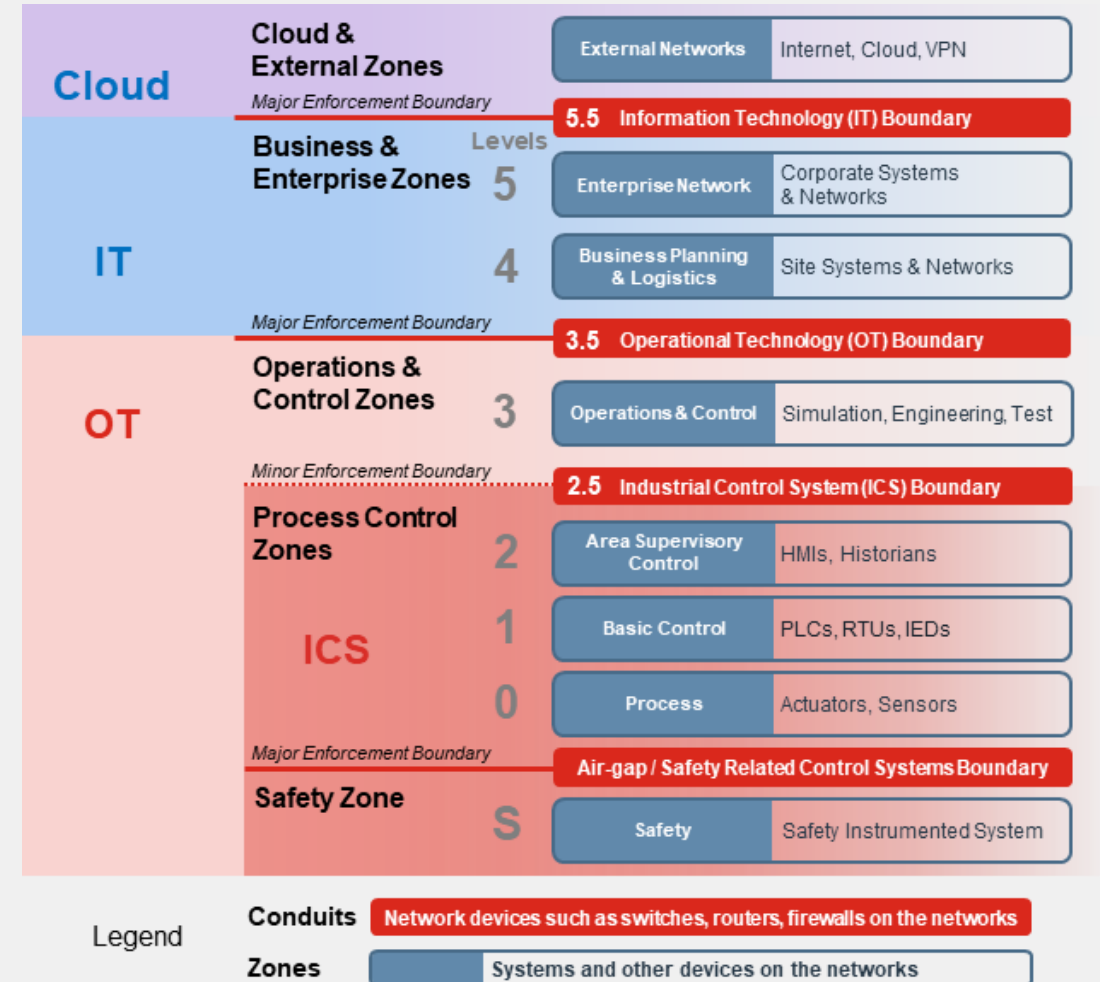


**Tech & Snack**

# OT Purdue Level View

## Purdue Level OT erklärt von CHATGPT

Das Purdue-Modell, auch bekannt als Purdue Enterprise Reference Architecture (PERA), ist ein Sicherheitskonzept für Operationstechnologie (OT). Es teilt OT-Systeme in verschiedene Ebenen oder Zonen auf, um die Sicherheit zu verbessern. Diese Ebenen umfassen die Prozessebene, die Produktionsleitebene, die übergeordnete Leitebene und die Unternehmensebene. Durch die Strukturierung und Trennung der OT-Infrastruktur sollen Sicherheitsrisiken minimiert und Angriffe erschwert werden. Das Purdue-Modell wird in der industriellen Automatisierung und OT-Sicherheit als bewährte Praxis angesehen.

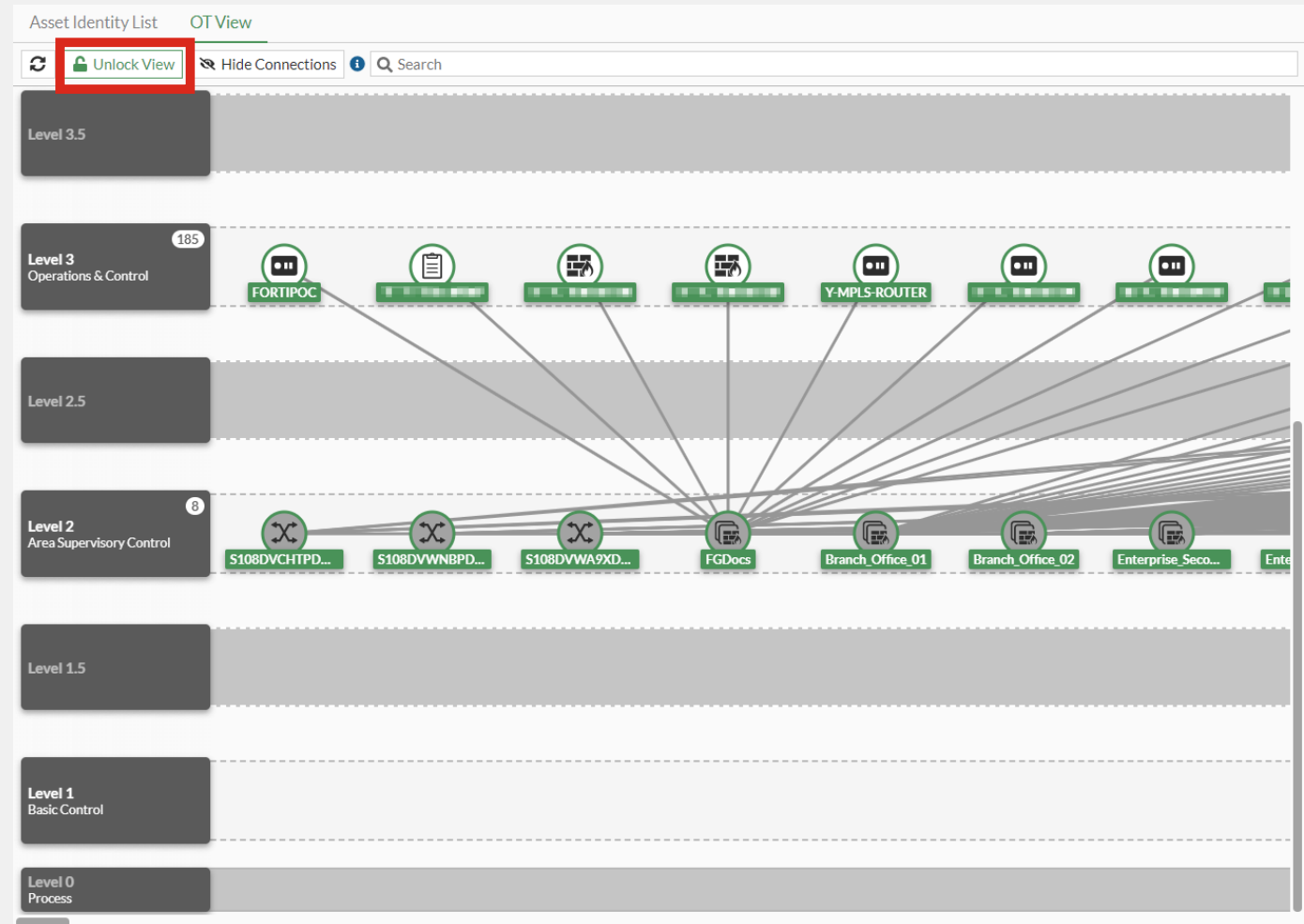


# OT Purdue Level View

*Security Fabric > Asset Identity Center*

Select: OT View tab

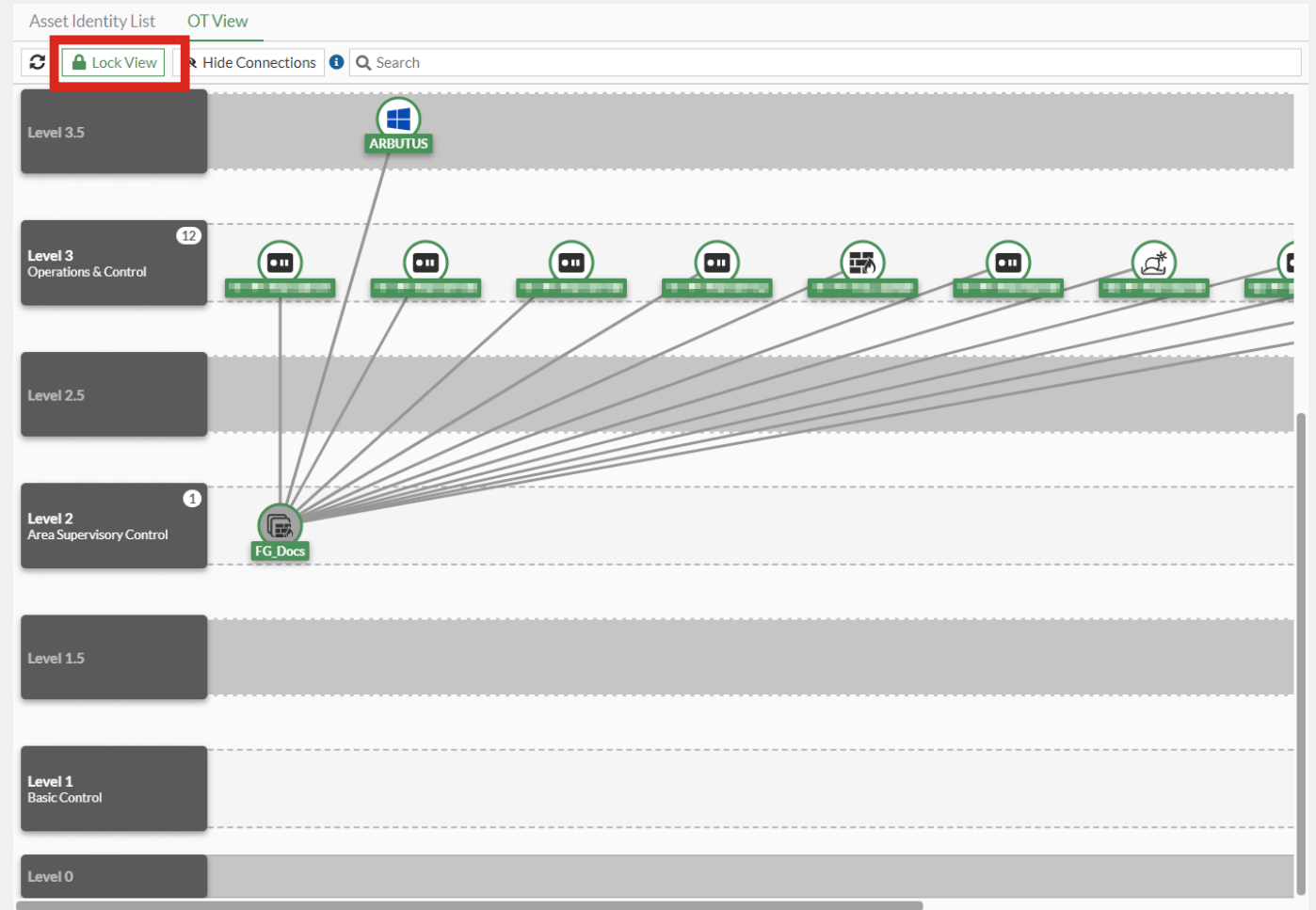
*Visualize network assets in Purdue Level based network topology and understand whether the security zones and conduits are implemented correctly and operating as intended.*



# OT Purdue Level View

Einzelne System anpassen

«Drag and Drop» Bearbeitung



# OT Purdue Level View

Einzelne Systeme anpassen









Security Fabric > Asset Identity Center

Asset Identity ListOT View

Show in OT View

Search

LatestAssetIdentity

| Device                                                                                          | Software OS             | Hardware                | FortiClient User | User | Status                                                                                     | Purdue Level                                                                                                                                | Vulnerabilities | Endpoint Tags |
|-------------------------------------------------------------------------------------------------|-------------------------|-------------------------|------------------|------|--------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|-----------------|---------------|
|                | Other identified device | Other identified device |                  |      |  Online | 3                                                                                                                                           |                 |               |
|                | Other identified device | Other identified device |                  |      |  Online | 3                                                                                                                                           |                 |               |
|  ARBUTUS       | Windows                 | Other identified device |                  |      |  Online | <div><div>3</div><div>5.5</div><div>5</div><div>4</div><div>3.5</div><div>3</div><div>2.5</div><div>2</div><div>1.5</div><div>1</div></div> |                 |               |
|  Y-MPLS-ROUTER | Other identified device | Other identified device |                  |      |  Online |                                                                                                                                             |                 |               |

CLI

|                                                                             |                                                            |
|-----------------------------------------------------------------------------|------------------------------------------------------------|
| # diagnose user-device-store device memory ot-purdue-set <mac> <ip> <level> |                                                            |
| mac                                                                         | Enter the MAC address of the device.                       |
| ip                                                                          | Enter the IPv4 address of the device.                      |
| level                                                                       | Enter the Purdue Level: 1, 1.5, 2, 2.5, 3, 3.5, 4, 5, 5.5. |



# OT Purdue Level View

## Interface Konfigurieren

### CLI

Der Default Purdue Level kann mittels CLI auf dem Interface gesetzt werden. (default-purdue-level)

Somit wird automatisch der Default Purdue Level der Systeme gesetzt.

Dieses Feature benötigt eine FortiGuard Industrial Security Service (ISS) Lizenz auf der FortiGate, damit Industrial Database (ISDB) benutzt werden kann. Damit dies funktioniert, muss Device Identification auf dem Interface aktiviert sein.

```
config system interface
 edit <name>
 set device-identification enable
 set default-purdue-level {1 | 1.5| 2 | 2.5| 3 | 3.5 | 4 | 5 | 5.5}
 next
end
```

Default Purdue Level ist 3.

Wenn der Wert auf dem Interface angepasst wird, werden alle Systeme an dem Interface auf den neuen Wert angepasst.

Falls aber schon ein Device gesetzt wurde (GUI oder CLI), wird diese Einstellung preferenziert.



# **FORTINET COMMUNITY**



## Fortinet Community

(<https://community.fortinet.com>)

The community is a place to collaborate, share insights and experiences, and get answers to questions

Requirements:

Only a FortiCloud (free) Account is required to login to the community

FuseCommunity was deprecated and finally replaced by the new community board



The screenshot shows the Fortinet Community website. At the top, there's a navigation bar with the Fortinet logo, 'Community', and links for 'Help' and a user profile. Below this, there are tabs for 'Forums', 'Knowledge Base', and 'Community Groups'. The main banner features a city street scene with the text 'Welcome to the Fortinet Community!' and a subtext: 'The community is a place to collaborate, share insights and experiences, and get answers to questions. Search here or look around to get started.' Below the banner is a search bar with a 'Community' dropdown and a 'Search here' input field. Three statistics are displayed: 54041 Discussions, 82043 Community Members, and 1311 Online Members. The 'Top Community Conversations' section is visible, with a 'Sort By' dropdown and tabs for 'Recent', 'Unanswered', 'Unsolved', and 'Solved'. A specific conversation is shown with a warning: 'Warning: Signature is missing or invalid.' and details about the post and replies.



# AGORA – AGORAWHAT?

The agora (/ˈæɡərə/; Ancient Greek: ἀγορά, romanized: agorá, meaning "market" in Modern Greek) was a central public space in ancient Greek city-states. It is the best representation of a city-state's response to accommodate the social and political order of the polis. The literal meaning of the word "agora" is "gathering place" or "assembly". The agora was the center of the athletic, artistic, business, social, spiritual, and political life in the city. The Ancient Agora of Athens is the best-known example.

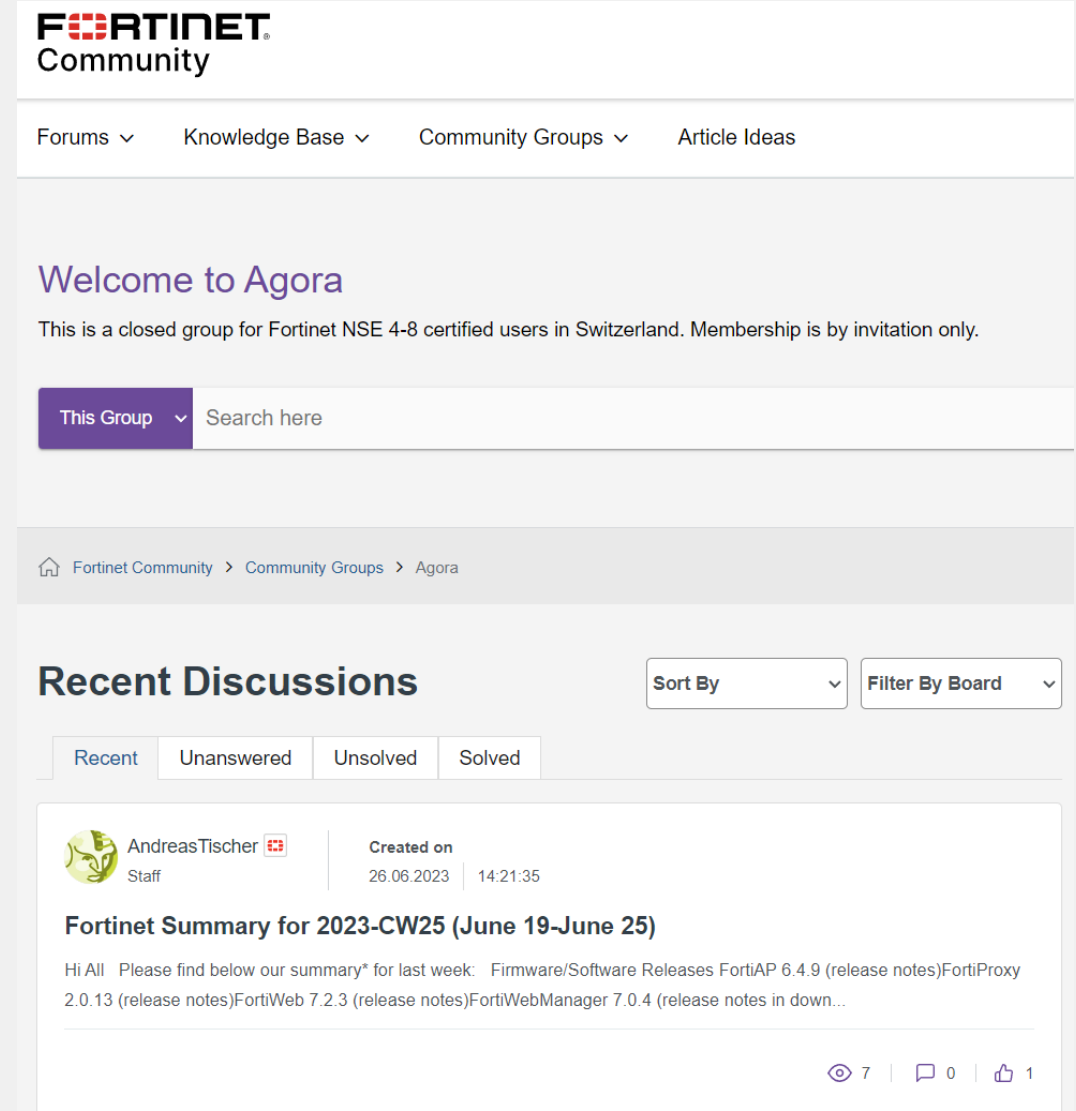


# AGORA – Where and what to find...

<https://community.fortinet.com/t5/Agora/cmp-p/grouphub:agora>

→ Login → Community Groups → Local Groups → AGORA

- Weekly Tech Update Newsletter for FTNT Employees, NSE4-certified Partners and Distribution
- Planned Release: every Monday – Tuesday
- Content: SW & HW Releases, newly and updated KBs, Videos, Soundcloud Content, EOS - EOL - EOO Information, Threat Information, Blogs, planned Events, Event-recordings, Product Specification Updates and more...
- Monthly Product Guide and HW Schematics Uploads with „handmade“ Change Logs (Yes, it's crazy but they like it)



The screenshot shows the Fortinet Community website interface. At the top is the Fortinet logo and 'Community' text. Below it are navigation links: Forums, Knowledge Base, Community Groups, and Article Ideas. The main heading is 'Welcome to Agora', followed by a note: 'This is a closed group for Fortinet NSE 4-8 certified users in Switzerland. Membership is by invitation only.' There is a search bar with a dropdown menu set to 'This Group'. Below this is a breadcrumb trail: Fortinet Community > Community Groups > Agora. The 'Recent Discussions' section features a 'Sort By' dropdown and a 'Filter By Board' dropdown. A list of discussion filters (Recent, Unanswered, Unsolved, Solved) is shown. The first discussion is titled 'Fortinet Summary for 2023-CW25 (June 19-June 25)' by staff member AndreasTischer, created on 26.06.2023 at 14:21:35. The discussion content mentions firmware/software releases for FortiAP 6.4.9, FortiProxy 2.0.13, FortiWeb 7.2.3, and FortiWebManager 7.0.4. At the bottom right of the discussion card, there are icons for views (7), replies (0), and likes (1).





**FRAGT UNS... ???**

Unsere Email : [security-ch@also.com](mailto:security-ch@also.com)

Unser Wiki: <https://fortinet.also.ch/wiki>

# THANK YOU

